***Listing of the Claims*:**

1. (Currently Amended) A system to provide application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another, the system comprising:

a first computer comprising a security application program interface and an application program interface coupled to a client application on a first platform, the security application program interface operable to provide a security credential;

an authentication authority receiving the security credential from the security application program interface, the authentication authority further generates a token and communicates the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent string data type;

a store maintaining data validating the security credential, the store in communication with the authentication authority to validate the security credential,

the application program interface communicating regarding the validity of the token; and

a second computer comprising a distinct server application on a second platform to receive the token from the application program interface, the server application communicating with the authentication authority to validate the

token to enable the client application to use services of the server application, wherein there is no continuing context or session and a new context is created with an invocation of the distinct server application by the client application.

2. (Previously Presented) The system of Claim 1, wherein the server application further comprises:

an application program interface to communicate with the application program interface of the client application; and

a security application program interface to communicate with the authentication authority.

3. (Previously Presented) The system of Claim 1, wherein the server application caches the token after validating the token with the authentication authority such that when the client application requests service of the server application, via the application program interfaces of the client application, the server application uses the cached token to validate the client application.

4. (Original) The system of Claim 1, wherein the token generated by the authentication authority comprises a string including at least a portion of the security credential.

5. (Original) The system of Claim 4, wherein at least a portion of the token is in Extensible Markup Language format.

6. (Original) The system of Claim 4, wherein at least a portion of the token is in Security Assertion Markup Language format.

7. (Original) The system of Claim 4, wherein the token includes information related to an expiration date of the token.

8. (Original) The system of Claim 1, wherein validating the token by the authentication authority includes determining whether the authentication authority created the token.

9. (Currently Amended) A method for providing application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another, the method comprising:

coupling a security application program interface and an application program interface to a client application on a first platform;

communicating a security credential from the security application program interface to an authentication authority;

communicating information related to the security credential between the authentication authority and a data store to determine whether the security credential is valid;

generating a token by the authentication authority when the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent string data type;

communicating the token to the client application;

providing, by the application program interface coupled to the client application on the first platform, the token to a distinct server application, the distinct server application on a second platform, wherein there is no continuing context or session and a new context is created with an invocation of the distinct server application by the client application; and

validating, by the server application, the token before providing access to services of the distinct server application by the client application.

10. (Previously Presented) The method of Claim 9, wherein the distinct server application is provided with a security application program interface coupled to the distinct server application for validating the token with the authentication authority.

11. (Previously Presented) The method of Claim 9, wherein the application program interface coupled to the client application communicates the token to an application program interface of the distinct server application.

12. (Previously Presented) The method of Claim 9, wherein validating the token by the distinct server application further comprises:

communicating information related to the token to the authentication authority;

determining, by the authentication authority, whether the token is authentic; and

receiving validation related information from the authentication authority.

13. (Currently Amended) The method of Claim 12, wherein the information related to the token [[is]] comprises the token.

14. (Currently Amended) The method of Claim 12, wherein the information related to the token [[is]] comprises a portion of data ~~comprising~~ included in the token.

15. (Original) The method of Claim 12, wherein the authentication authority determines whether the authentication authority generated the token to validate the token.

16. (Original) The method of Claim 15, wherein the authentication authority determines whether the token has expired.

17. (Original) The method of Claim 12, wherein the authentication authority determines whether the token has expired.

18. (Original) The method of Claim 9, wherein the token includes a portion of the security credential in a string format.

19. (Original) The method of Claim 18, wherein the token includes at least an information related to an expiration date of the token.

20. (Original) The method of Claim 18, wherein the token is encrypted.

21. (Original) The method of Claim 18, wherein the string format of the token is further defined as an Extensible Markup Language format.

22. (Original) The method of Claim 18, wherein the string format of the token is further defined as Security Assertion Markup Language format.

23. (Previously Presented) The method of Claim 9, wherein the client further includes the application program interface coupled to the client application for communicating with the server application and wherein the client further includes the security

application program interface coupled to the client application to communicate with the authentication authority.

24. (Original) The method of Claim 9, wherein the security credential is further defined as including a password and user identification.

25. (Original) The method of Claim 24, wherein the security credential is further defined as encrypted and the data store is further defined as a data store maintaining user identifications and passwords.

26. (Original) The method of Claim 9, wherein the security credential is an X.509 certificate and the data store is a certificate authority.

27. (Original) The method of Claim 26, further comprising:

communicating the X.509 certificate from the authentication authority to the certificate authority;

validating the X.509 certificate by the certificate authority; and

communicating validation information to the authentication authority.

28. (Currently Amended) A system to provide application-to-application enterprise security for different applications on different platforms where there is no continuing context or session and a new context is created with new invocations from one of the applications to another, the system comprising:

a first computer comprising a first application program interface coupled to a first application on a first platform and a first security application program interface coupled to the first application on the first platform, to provide a first security credential;

~~a first security application program interface coupled to the first application on the first platform, to provide a first security credential;~~

a second computer comprising a second application program interface coupled to a second application on a second platform and a second security application program interface coupled to the second application on the second platform, to provide a second security credential;

~~a second security application program interface coupled to the second application on the second platform, to provide a second security credential;~~

an authentication authority receiving the first and second security credentials from the first and second security application program interfaces, the authentication authority further generating tokens and communicating the tokens to the first and second security application program interfaces where the first and second security credentials are valid, wherein the token contains user credentials encoded as a platform and application

independent string data type, wherein the tokens generated by the authentication authority are further defined as a first token generated by the authentication authority for the first application based on the first security credential and a second token generated by the authentication authority for the second application based on the second security credential;

a store maintaining data validating the first and second security credentials, the store in communication with the authentication authority to validate the first and second security credentials;

the first application program interface communicating regarding tokens; and

the second application program interface receiving the first token from the first application program interface, wherein there is no continuing context or session and a new context is created with an invocation of the second application program interface by the first application program interface, the second security application program interface communicating with the authentication authority to validate the first token to enable the first application to use services of the second application and wherein the ~~second~~ first application program interface receives the second token from the second application program interface, wherein there is no continuing context or session and a new context is created with an invocation of the first application program interface by the second application program interface, the first security application program interface communicating with the authentication authority to validate the second token to enable the second application to use services of the first application.

29. (Canceled)

30. (Original) The system of Claim 28, wherein the first and second tokens are further defined as data provided in a string format including at least portions of the first and second security credentials, respectively.

31. (Previously Presented) The system of Claim 30, wherein the first and second tokens include an expiration date.

32. (Original) The system of Claim 30, wherein the string format of the first and second tokens is further defined as Extensible Markup Language Format.

33. (Original) The system of Claim 30, wherein the string format of the first and second tokens is further defined as Security Assertion Markup Language Format.